様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月　 ３ 日現在

機関番号：１４４０１
研究種目：若手研究
研究期間：2021～2023
課題番号：２１Ｋ１７７４２

研究課題名（和文）確率モデルに基づく最適なセキュリティパッチ管理ツールの開発

研究課題名（英文）Optimal security patch management tool design based on probabilistic modeling and analysis

研究代表者
鄭　俊俊（Zheng, Junjun）

大阪大学・大学院情報科学研究科・特任助教（常勤）

研究者番号：８０８２２８３２

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：本研究では，耐侵入システムの最適なパッチ適用戦略を確率モデルに基づいて検討し，セキュリティパッチ管理ツールを開発した．システムの振る舞いをマルコフ再生過程を用いてモデル化し，セキュリティ評価とコスト評価の両観点から最適なパッチ適用タイミングを明らかにした．また，感度分析を行うことで，システムの最適化を図った．深層学習でマルウェアの検出と分類方法を提案し，システムの安全性と可用性を向上させた．さらに，階層的モデリングで多状態システムの性能指標の評価方法を提案し，異なる視点から最適なパッチ適用戦略の策定を可能にした．この研究は耐侵入システムの理論基盤を強化し，実用化への重要なステップとなった．

研究成果の学術的意義や社会的意義
本研究は，耐侵入システムの理論的基盤を強化し，最適なセキュリティパッチ管理を実現するための新しいアプローチを提供した点で学術的意義がある．確率モデルと深層学習を組み合わせることで，システムの信頼性と安全性を向上させる手法を確立した．また、これによりシステム管理者がより効率的にセキュリティパッチを適用できるようになり，サイバー攻撃に対する防御力が向上する社会的意義も大きい．実用化に向けた重要なステップを踏み出した本研究は，セキュリティ技術の発展に寄与している．

研究成果の概要（英文）：This study focuses on developing an optimal security patch management tool for intrusion-tolerant systems using probabilistic models. The system behavior is modeled using Markov regenerative processes, and the optimal patch application timing is determined from both security and cost perspectives. Sensitivity analysis is conducted to optimize the system design by identifying parameters that significantly impact system reliability and performance. Additionally, deep learning techniques are employed to propose efficcient methods for malware detection and classification, enhancing system safety and availability. A hierarchical modeling approach is proposed for calculating performance measures for multi-state systems, enabling the determination of optimal patch application strategies from various performance perspectives. This study strengthened the theoretical foundation of intrusion-tolerant systems and marked a significant step towards practical implementation.

研究分野：情報学

キーワード：耐侵入システム　確率モデル　マルコフ再生過程　位相型近似　感度分析　パッチ管理

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

(1) 学術的背景

近年，情報システムへの侵入（不正アクセス）は増え続けており，悪意のある攻撃が随所で発生するようになったため，そのような攻撃を防ぐことはかつてないほど難しくなっている．そのため，ネットワークに接続されたパソコンや携帯電話などの端末のセキュリティ対策として，効率的なパッチ管理戦略が防御の第一歩となりつつある．大きなセキュリティ事故の主な原因は，システムが内包する脆弱性である．脆弱性は，悪意のある者がコンピュータシステムに関して許可されている以上のアクセスや特権を得るために，悪用する可能性があることが欠陥である．セキュリティパッチを適用することで脆弱性を修正できる．パッチとは，ソフトウェア内の脆弱性を解決するために開発された追加コードである．一般に，セキュリティ問題に対するタイムリーなパッチ適用は，情報システムの運用の可用性，機密性および完全性を維持するために不可欠なものである．しかし，セキュリティ・ＩＴ専門家が指摘しているように，ユーザが必ずしもパッチを適切に適用しているとは限らないことが課題である．新しいパッチは日々リリースされているが，経験豊富なシステム管理者でさえ，全てのパッチをタイミングよく適切に導入することは困難である．また，パッチを適用することでシステムが不具合になって停止する可能性もある．

一方で，システムの振る舞いをモデル化し，システムが正しく動作することを定量的に検証することが重要である．一般に，状態依存型のモデル化手法の一つであるマルコフ連鎖が使われることが多い．しかし，マルコフ連鎖は状態間の推移時間が仮定されているので，リアルタイムシステムなどのように確定的な時間内での処理制約があるようなシステムの振る舞いを正確に表現することができない．これを解決するために，状態遷移時間を一般分布で表現することが必要となる．

(2) 解決すべき課題

本研究ではマルコフ再生過程（MRGP: Markov Regenerative Process）と呼ばれる確率点過程に着目する．MRGP は一般分布による状態遷移を含むので，非マルコフモデルとも呼ばれ，通常のマルコフ連鎖やセミマルコフ過程などを包括する一般的な点過程である．MRGP に対する過渡解析は定常解析よりも困難であり，一般分布を何らかの近似によって表現することが必要となる．本研究では，位相型近似（Phase-Type Approximation）を考える．位相型近似は一般分布を位相型分布などのマルコフ連鎖で記述される確率分布で置き換える手法であり，MRGP の過渡解析を実現するための有力な手法として位置づけられている．MRGP を用いて耐侵入システムの振る舞いを表現する．また，位相型近似により MRGP の過渡解析と定常解析を行い，システムセキュリティとコストの両方の観点から最適なセキュリティパッチ管理戦略の提案とその有効性の検証を目指す．

２．研究の目的

(1) 研究課題の目的と特徴

本研究では，耐侵入システムのセキュリティの向上を目的として，最適なパッチ管理戦略の考案とその有効性の検証を行う．

MRGP の定常解析は隠れマルコフ連鎖（EMC: Embedded Markov chain）解析に帰着されることが多い．MRGP の定常解析と比べて過渡解析のほうが極端に難しくなる．実際，ラプラス・スティルチェス変換（LST: Laplace-Stieltjes Transform）に対して逆変換を行うことで，システムの過渡状態確率を求めることができるが，LST の数値変換は不安定であり，変換における丸め誤差や打切り誤差を制御できないことが明らかにされていた．

(2) 期待される効果

本研究では，一般分布に対して位相型近似を行うことで MRGP を連続時間マルコフ連鎖（CTMC: Continuous-Time Markov Chain）として近似できる．さらに，CTMC 解析により定常解のみならず過渡解も得ることができる．これは従来まで考えられていた EMC や LST の逆変換の概念ではなく，より精度が高く効率のよい MRGP に対する過渡解析を行えることが期待される．一方で，本研究はシステムのモデル化だけではなく，脆弱性の発見によるセキュリティ脅威を不正アクセス発生率と紐付け，パッチ管理の観点から耐侵入システムにおけるセキュリティ評価とコスト評価を行い，実用的な観点から評価を行う．

また，提案したパッチ管理戦略の有効性を数値シミュレーションを通じて検証する．システムの

動的な振る舞いとパッチ管理戦略の効果を詳細に解析し，セキュリティ評価とコスト評価を行う．これにより，実際の運用環境での適用可能性を評価する．

３．研究の方法

(1) 耐侵入システムの最適なセキュリティパッチ管理戦略の提案

① システムのモデル化：耐侵入システムの振る舞いをマルコフ再生過程（MRGP）によって表現し，MRGP の状態遷移が不明確な場合には確率報酬ネット（SRN: Stochastic Reward Net）から導出する．SRN は確率ペトリネットに報酬を考慮したモデルで，一般発火（発火遅延が一般分布で記述される）を用いることで高い表現能力を持つ．これにより，システムの動的な振る舞いを正確にモデル化する．

② クロネッカー表現による位相型近似の適用：一般分布を近似する手法である位相型近似を用い，MRGP を連続時間マルコフ連鎖に還元する．クロネッカー和・積を用いることで状態数を低減し，連続時間マルコフ連鎖の無限小生成行列を生成する．これにより，システムの解析を効率化し，実用的な解析手法を提供する．

③ 過渡解析および定常解析による評価：連続時間マルコフ連鎖の無限小生成行列を用いて，過渡解析および定常解析を行う．各状態の報酬値を考慮し，システム可用性の観点からセキュリティレベルを算出する．また，各状態の滞在時間を用いてパッチ適用コストやメンテナンスコストを評価することで，経済的な側面も考慮した最適なパッチ管理戦略を導出する．

④ 最適なパッチ管理戦略の確立：複数のパッチ管理戦略を提案し，過渡解析および定常解析の結果をもとに，システムのセキュリティレベルとコストの両面から最適なパッチ管理戦略を決定する．これにより，実用的で効果的なセキュリティパッチ管理手法を確立する．

(2) 研究成果の応用と検証

① 数値シミュレーションによる検証：提案したパッチ管理戦略の有効性を確認するために，数値シミュレーションを実施する．システムの動的な振る舞いとパッチ管理戦略の効果を詳細に解析し，実際の運用環境での適用可能性を評価する．

② モデルの改良：数値シミュレーションの結果をもとに，モデルの精度や適用性を向上させるための改良を行う．これには，システムのパラメータ調整や新しいモデリング手法の導入が含まれる．

③ 学術的発信：研究成果を国内外の学会やジャーナルで発表し，研究の位置づけとインパクトを確認する．これにより，他の研究者との情報交換や共同研究の機会を拡大し，研究成果の実用化に向けた基盤を築く．

４．研究成果

令和 3 年度は主に仮想化型耐侵入システムの確率モデルの構築と性能評価を行った．具体的には，仮想型耐侵入システムに対する確率モデルをマルコフ到着過程に基づいて構築し，待ち行列理論の行列解析法を用いてシステム信頼性を定式化した．セキュリティ障害時間分布の LS（Laplace-Stieltjes）変換から平均セキュリティ障害時間（MTTSF: Mean Time to Security Failure）を導出し，Durbin 法や Gaver 法などの逆ラプラス変換を適用して具体的な障害時間分布を評価する手法を確立した．この成果は，セキュリティパッチ管理のタイミングにおける理論的基盤を提供し，セキュリティ管理手法の高度化に寄与する．また，システムの振る舞いを確率報酬ネット（SRN）で表現し，マルコフ再生過程モデルを導出することで，定常解析によるシステムの可用性評価を行った．位相型近似を用いた解析により，具体的な可用性指標を求める手法を開発した．この手法は，システムの長期的な信頼性と可用性の評価に役立ち，セキュリティシステム設計の指針となる．なお，DoS 攻撃に対する予防保守を伴う耐侵入システムの過渡的な振る舞いをセミマルコフモデルで記述し，システムの信頼性と可用性の統一的な評価指標である区間信頼性（Interval reliability）を解析的に定式化した．稼働時間が指数分布に従う場合の区間信頼性を最大化する最適な予防保守方策を導出し，数値例を用いて具体的な最適方策を示した．この成果は，実際のシステム運用におけるセキュリティ対策の効率化に大きなインパクトを与える．

さらに，MRGP の感度分析手法を開発した．マルコフ再生過程は数理的に解析できるクラスの中で最も高い表現力を持つため，システムの信頼性評価において広く利用されている．しかし，マルコフ再生過程の状態遷移モデルは再生状態と非再生状態を持つため，解析を行うことは必ずしも容易ではない．一方，感度解析は，モデルにおける入力因子（パラメータ）の変化がモデル出力に与える影響を定量化する手法である．本研究では，マルコフ再生過程の定常解に着目し，定常解に対する感度分析の手法を提案した．特に，隠れマルコフ連鎖の手法を用いて定常解析を行い，モデルパラメータの感度を定式化した．感度分析によりシステムの信頼性に大きく影響するパラメータやコンポーネントを明らかにし，有効な改善策を提案した．この手法は，システム

の設計および運用における重要なツールとなる．

令和 4 年度と 5 年度は主に最適なパッチ管理戦略の決定とその有効性の検証を行った．具体的には，DoS 攻撃に対する予防保守を伴う耐侵入システムの過渡的振る舞いに焦点を当て，確率的フレームワークを用いてシステムの可用性を評価した．特に，プル型パッチ管理（Pull-type security management）を行う ITS の動的挙動を捉える複合確率報酬ネット（SRN）を開発し，脆弱性の発見、侵入耐性、反応保守操作をモデル化した．また，位相型近似を用いてマルコフ再生過程（MRGP）モデルを解き，区間可用性と定常可用性の二種類の可用性基準を定式化した．数値実験により，脆弱性チェック間隔の変化がシステム可用性への影響を明らかにし，プル型セキュリティパッチ管理方策の有効性について論じた．さらに，システムの可用性の観点に限らず，セミマルコフと LS 変換を用いて，耐侵入システムの区間信頼性という評価指標の算出方法を提案した．この研究は，現実のシステムおけるパッチ管理の実効性を高める．また，システムの最適化においては，新しい感度分析理論を開発し，これを解析的手法と組み合わせることで，より効果的な設計が可能となった．モデルパラメータの感度分析を通じて，システムコンポーネントの重要度を評価する方法を探求した．さらに，深層学習の技術が進展する中，これをサイバーセキュリティへ応用する試みを行い，システムの安全性向上に貢献した．特に，深層学習技術を活用し，システムのセキュリティに悪い影響を及ぼすマルウェアの検出および分類方法を提案した．これにより，セキュリティパッチの適用前に潜在的な脅威を迅速かつ正確に特定し，より効果的なパッチ管理方策を開発することが可能となった．加えて，階層的モデリングを用いることで，多状態システムを活用し，性能評価のための新たな指標を計算する手法を提案した．このアプローチにより，システムの可用性およびセキュリティ性能の向上を目指す最適なパッチ適用戦略を策定することが可能となった．

本研究を通じて，耐侵入システムの理論的基盤を強化し，実際のセキュリティ環境での応用に向けた基盤を築くことができた．耐侵入システムの開発と評価における新しいアプローチを提供することで，将来のセキュリティ技術の進化に貢献することを目指している．

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Junjun Zheng, Hiroyuki Okamura, and Tadashi Dohi	４．巻 -
２．論文標題 Sensitivity analysis for a Markov regenerative software rejuvenation model	５．発行年 2022年
３．雑誌名 Stochastic Models	６．最初と最後の頁 1〜28
掲載論文のDOI（デジタルオブジェクト識別子） 10.1080/15326349.2022.2117195	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Junjun Zheng, Hiroyuki Okamura, Tadashi Dohi, and Kishor S. Trivedi	４．巻 70
２．論文標題 Quantitative Security Evaluation of Intrusion Tolerant Systems With Markovian Arrivals	５．発行年 2021年
３．雑誌名 IEEE Transactions on Reliability	６．最初と最後の頁 547〜562
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TR.2020.3026570	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Junjun Zheng, Hiroyuki Okamura, and Tadashi Dohi	４．巻 9
２．論文標題 Availability Analysis of Software Systems with Rejuvenation and Checkpointing	５．発行年 2021年
３．雑誌名 Mathematics	６．最初と最後の頁 846〜846
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/math9080846	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計8件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 Junjun Zheng, Hiroyuki Okamura, and Tadashi Dohi
２．発表標題 On the interval reliability of intrusion tolerant systems using semi-Markov models
３．学会等名 The 10th Asia-Pacific International Symposium on Advanced Reliability and Maintenance（国際学会）
４．発表年 2022年

１．発表者名
Junjun Zheng, Hiroyuki Okamura, and Tadashi Dohi

２．発表標題
A note on optimal pull-type security patch management policies for intrusion tolerant systems

３．学会等名
電子情報通信学会信頼性研究会

４．発表年
2022年

１．発表者名
Junjun Zheng, Hiroyuki Okamura, and Tadashi Dohi

２．発表標題
A note on Interval Reliability Analysis of Intrusion Tolerant Systems Subject to DoS Attacks

３．学会等名
電子情報通信学会信頼性研究会

４．発表年
2022年

１．発表者名
Chen Li, Zheng Chen, and Junjun Zheng

２．発表標題
An efficient transformer encoder-based classification of malware using API calls

３．学会等名
The 24th IEEE International Conference on High Performance Computing & Communications（国際学会）

４．発表年
2022年

１．発表者名
Junjun Zheng, Hiroyuki Okamura, and Tadashi Dohi

２．発表標題
Sensitivity Analysis of Software Rejuvenation Model with Markov Regenerative Process

３．学会等名
2021 IEEE International Symposium on Software Reliability Engineering Workshops（国際学会）

４．発表年
2021年

１．発表者名
Junjun Zheng, Hiroyuki Okamura, and Tadashi Dohi

２．発表標題
Interval Reliability Analysis of Intrusion Tolerant Systems Subject to DoS Attacks

３．学会等名
The 5th International Conference on Mathematical Techniques in Engineering Applications（国際学会）

４．発表年
2021年

１．発表者名
Junjun Zheng, Hiroyuki Okamura, and Tadashi Dohi

２．発表標題
A Note on Sensitivity Analysis of Software Rejuvenation Model with Markov Regenerative Process

３．学会等名
電子情報通信学会信頼性研究会

４．発表年
2021年

１．発表者名
Junjun Zheng, jiahao Zhang, Hiroyuki Okamura, and Tadashi Dohi

２．発表標題
A Note on Local Sensitivity Analysis of Stationary Solutions for Markov Regenerative Processes

３．学会等名
電子情報通信学会信頼性研究会

４．発表年
2021年

〔図書〕　計1件

１．著者名 Junjun Zheng, Hiroyuki Okamura, and Tadashi Dohi	４．発行年 2023年
２．出版社 IntechOpen	５．総ページ数 20
３．書名 Maintenance Management - Current Challenges, New Developments, and Future Directions (Chapter 5: Pull-type security patch management in intrusion tolerant systems: modeling and analysis) (G. Lambert-Torres et al., eds.)	

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関